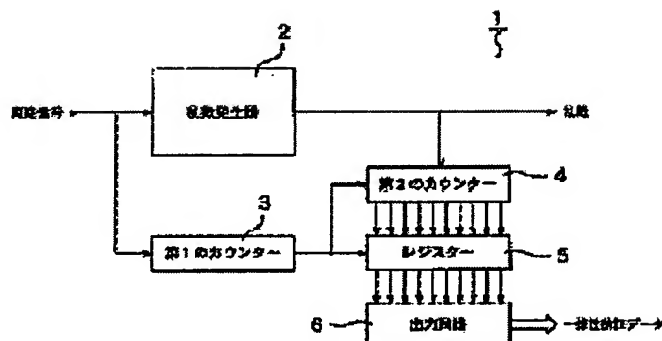


# 1-BIT RANDOM NUMBER GENERATOR, MULTI-BIT RANDOM NUMBER GENERATOR AND PROBABILITY GENERATOR

Patent number: JP2003029963  
 Publication date: 2003-01-31  
 Inventor: YAMAMOTO HIROYASU; SHIGA TAKAAKI; SHIMIZU TAKAKUNI; KOIBUCHI MISAKO  
 Applicant: FDK CORP  
 Classification:  
 - International: G06F7/58; G09C1/00  
 - european:  
 Application number: JP20010216704 20010717  
 Priority number(s): JP20010216704 20010717

## Abstract of JP2003029963

**PROBLEM TO BE SOLVED:** To easily verify the appearance uniformity of random number data and to improve reliability in a random number generator and a probability generator utilized in scientific and technical calculations or the like. **SOLUTION:** The random number generator 2 outputting '1' and '0' as the random number data is provided with a first counter 3 counting the fixed number of times and a second counter 4 counting the number of times of the appearance of the random number data and generating the number-of-times data. A register 5 holds the number-of-times data of the second counter 4 for each cycle counted in the first counter 3 and an output circuit 6 outputs the number-of-times data held in the register 5 as verification data. Thus, the appearance uniformity of the random number data can be verified by itself and the need that a user perform a statistic processing is eliminated.



Data supplied from the esp@cenet database - Worldwide

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2003-29963  
(P2003-29963A)

(43)公開日 平成15年1月31日(2003.1.31)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	特許出願公開番号
G 0 6 F 7/58		C 0 6 F 7/58	A 5 J 1 0 4
G 0 9 C 1/00	6 5 0	C 0 9 C 1/00	6 5 0 B

審査請求 有 請求項の数11 O L (全 16 頁)

(21)出願番号 特願2001-216704(P2001-216704)

(22)出願日 平成13年7月17日(2001.7.17)

(71)出願人 00023/721

エフ・ディ・ケイ株式会社  
東京都港区新橋5丁目36番11号

(72)発明者 山本 博康

東京都港区新橋5丁目36番11号 いわき電  
子株式会社内

(72)発明者 志賀 隆明

東京都港区新橋5丁目36番11号 いわき電  
子株式会社内

(74)代理人 10006/046

弁理士 尾股 行雄 (外1名)

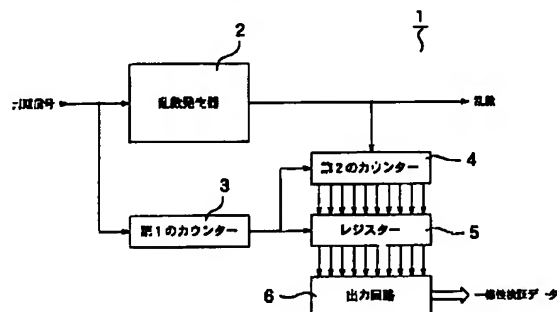
最終頁に続く

(54)【発明の名称】 1ビット乱数発生装置および多数ビット乱数発生装置ならびに確率発生装置

(57)【要約】

【課題】 科学技術計算などに利用される乱数発生装置および確率発生装置において、乱数データの出現一様性を手軽に検証して信頼性を高める。

【解決手段】 乱数データとして「1」と「0」を出力する乱数発生器2に、一定回数を計数する第1のカウンタ3と、乱数データの出現回数を計数して回数データを生成する第2のカウンタ4とを備える。第1のカウンタ3で計数された周期ごとに第2のカウンタ4の回数データをレジスタ5が保持し、レジスタ5に保持された回数データを出力回路6が検証データとして出力する。これにより、乱数データの出現一様性を自ら検証でき、使用者が統計処理を行う必要がなくなる。



【特許請求の範囲】

【請求項1】 乱数データとして「1」と「0」を出力する乱数発生器(2)を有し、一定回数を計数する第1のカウンター(3)と、前記乱数発生器から出力された乱数データの出現回数を計数して回数データを生成する第2のカウンター(4)とを備え、第1のカウンターで計数された周期ごとに第2のカウンターの回数データを保持するレジスター(5)を備え、このレジスターに保持された回数データを検証データとして出力する出力回路(6)を備えたことを特徴とする1ビット乱数発生装置。

【請求項2】 出力回路(6)に代えて、予め設定された上限比較データおよび下限比較データとレジスター(5)に保持されたデータとを比較して検証信号を出力する比較器(7)を備えたことを特徴とする請求項1に記載の1ビット乱数発生装置。

【請求項3】 乱数データとして「1」と「0」を出力する乱数発生器(2)を有し、この乱数発生器から出力された前回の乱数データを保持するデータ保持器(8)を備え、前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する比較器(9)を備え、前記比較器からカウントアップ信号を受けたときにカウントアップするとともに、前記比較器からカウントクリア信号を受けたときにカウントクリアするカウンター(10)を備え、このカウンターに保持されたデータを検証データとして出力する出力回路(6)を備えたことを特徴とする1ビット乱数発生装置。

【請求項4】 乱数データとして「1」と「0」を出力する乱数発生器(2)を有し、この乱数発生器から出力された前回の乱数データを保持するデータ保持器(8)を備え、前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する第1の比較器(11)を備え、第1の比較器からカウントアップ信号を受けたときにカウントアップするとともに、第1の比較器からカウントクリア信号を受けたときにカウントクリアするカウンター(10)を備え、このカウンターの出力データを保持するレジスター(12)を備え、このレジスターのデータと前記カウンターの出力データとを比較して、前者より後者の方が大きいときにデータ

上書き信号を出力するとともに、それ以外のときにデータ保持信号を出力する第2の比較器(13)を備え、第2の比較器からデータ上書き信号を受けたときに前記カウンターの出力データを前記レジスターに書き込むとともに、第2の比較器からデータ保持信号を受けたときに前記レジスターのデータを保持するように制御する制御回路(14)を備え、前記レジスターに保持されたデータを検証データとして出力する出力回路(15)を備えたことを特徴とする1ビット乱数発生装置。

【請求項5】 出力回路(15)に代えて、予め設定された比較データとレジスター(12)に保持されたデータとを比較して検証信号を出力する第3の比較器(16)を備えたことを特徴とする請求項4に記載の1ビット乱数発生装置。

【請求項6】 乱数データとして「1」と「0」を出力する乱数発生器(2)を有し、一定回数を計数する第1のカウンター(17)を備え、前記乱数発生器から出力された前回の乱数データを保持するデータ保持器(8)を備え、前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する比較器(9)を備え、前記比較器からカウントアップ信号を受けたときにカウントアップするとともに、前記比較器からカウントクリア信号を受けたときにカウントクリアする第2のカウンター(18)を備え、第2のカウンターの出力データをデコードして各信号長ごとに出力するデコーダー(19)を備え、このデコーダーの出力データを各信号長ごとにそれぞれカウントする複数の第3のカウンター(20)を備え、

第1のカウンターで計数された一定回数ごとに第3の各カウンターの出力データをそれぞれ保持する複数のレジスター(21)を備え、

第1のカウンターで計数された一定回数ごとの信号と前記比較器の出力データとに基づいて前記各レジスターから検証データを出力するように制御する制御回路(22)を備えたことを特徴とする1ビット乱数発生装置。

【請求項7】 レジスター(21)の出力データを選択して出力する選択回路(23)を付設したことを特徴とする請求項6に記載の1ビット乱数発生装置。

【請求項8】 請求項1または請求項3または請求項4または請求項6または請求項7に記載の1ビット乱数発生装置(1)を複数個並列に接続し、これら1ビット乱数発生装置から出力された検証データをビットごとに選択して出力する選択回路(26)を付設したことを特徴とする多数ビット乱数発生装置。

【請求項9】 請求項2または請求項5に記載の1ビット乱数発生装置(24)を複数個並列に接続し、これら1ビット乱数発生装置から出力された検証信号をビットごとに選択して出力する選択回路(27)を付設したことを特徴とする多数ビット乱数発生装置。

【請求項10】 請求項1から請求項7までのいずれかに記載の1ビット乱数発生装置(1、24)を有し、この1ビット乱数発生装置から出力された乱数データをシリアルデータからパラレルデータへ変換するシフトレジスタ(31)を備え、一定のパラレルデータのビット長を計数するカウンター(32)を備え、このカウンターで計数された周期ごとに前記シフトレジスタのパラレルデータを保持するレジスタ(33)を備え、予め設定された確率上限データおよび確率下限データと前記レジスタに保持されたパラレルデータとを比較して確率信号を出力する比較器(34)を備えたことを特徴とする確率発生装置。

【請求項11】 請求項8または請求項9に記載の多数ビット乱数発生装置(25)を有し、予め設定された確率上限データおよび確率下限データと前記多数ビット乱数発生装置から出力された乱数データとを比較して確率信号を出力する比較器(35)を備えたことを特徴とする確率発生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、科学技術計算、ゲーム機、或いは暗号化処理などに利用するに好適な1ビット乱数発生装置および多数ビット乱数発生装置と、これらを用いた確率発生装置に関するものである。

【0002】

【従来の技術】一般に、乱数発生器を備えた乱数発生装置(1ビット乱数発生装置、多数ビット乱数発生装置)や確率発生装置において、その製品としての信頼性を高めるためには、乱数発生器から送出される乱数データに前後関係、規則性、周期性がないことに加えて、この乱数データに出現一様性(乱数によって出現率に差異が生じないこと)があることが重要となる。そのため従来は、乱数発生器から連続的に送出された膨大な乱数データが使用者が統計処理してその出現一様性を検証していた。

【0003】

【発明が解決しようとする課題】しかし、これでは乱数データの統計処理が面倒で煩雑となるので、出現一様性の検証に手間がかかるという不都合があった。

【0004】本発明は、このような事情に鑑み、乱数データの出現一様性を手軽に検証して信頼性を高めることが可能な1ビット乱数発生装置および多数ビット乱数発生装置ならびに確率発生装置を提供することを目的とす

る。

【0005】

【課題を解決するための手段】本発明では、1ビット乱数発生装置および多数ビット乱数発生装置ならびに確率発生装置の製品としての信頼性を高めるべく、乱数データの出現一様性を自ら検証できる機能を内蔵することに着目した。

【0006】すなわち、本発明のうち請求項1に係る発明は、乱数データとして「1」と「0」を出力する乱数発生器(2)を有し、一定回数を計数する第1のカウンター(3)と、前記乱数発生器から出力された乱数データの出現回数を計数して回数データを生成する第2のカウンター(4)とを備え、第1のカウンターで計数された周期ごとに第2のカウンターの回数データを保持するレジスタ(5)を備え、このレジスタに保持された回数データを検証データとして出力する出力回路(6)を備えて構成される。

【0007】また、本発明のうち請求項2に係る発明は、上記出力回路(6)に代えて、予め設定された上限比較データおよび下限比較データと上記レジスタ(5)に保持されたデータとを比較して検証信号を出力する比較器(7)を備えて構成される。

【0008】また、本発明のうち請求項3に係る発明は、乱数データとして「1」と「0」を出力する乱数発生器(2)を有し、この乱数発生器から出力された前回の乱数データを保持するデータ保持器(8)を備え、前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する比較器(9)を備え、前記比較器からカウントアップ信号を受けたときにカウントアップするとともに、前記比較器からカウントクリア信号を受けたときにカウントクリアするカウンター(10)を備え、このカウンターに保持されたデータを検証データとして出力する出力回路(6)を備えて構成される。

【0009】また、本発明のうち請求項4に係る発明は、乱数データとして「1」と「0」を出力する乱数発生器(2)を有し、この乱数発生器から出力された前回の乱数データを保持するデータ保持器(8)を備え、前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する第1の比較器(11)を備え、第1の比較器からカウントアップ信号を受けたときにカウントアップするとともに、第1の比較器からカウントクリア信号を受けたときにカウントクリアするカウンター(10)を備え、このカウンターの出力データを保持するレジスタ(12)を備え、このレジスタのデータと前記カウン

ターの出力データとを比較して、前者より後者の方が大きいときにデータ上書き信号を出力するとともに、それ以外のときにデータ保持信号を出力する第2の比較器(13)を備え、第2の比較器からデータ上書き信号を受けたときに前記カウンターの出力データを前記レジスタに書き込むとともに、第2の比較器からデータ保持信号を受けたときに前記レジスタのデータを保持するように制御する制御回路(14)を備え、前記レジスタに保持されたデータを検証データとして出力する出力回路(15)を備えて構成される。

【0010】また、本発明のうち請求項5に係る発明は、上記出力回路(15)に代えて、予め設定された比較データと上記レジスタ(12)に保持されたデータとを比較して検証信号を出力する第3の比較器(16)を備えて構成される。

【0011】また、本発明のうち請求項6に係る発明は、乱数データとして「1」と「0」を出力する乱数発生器(2)を有し、一定回数を計数する第1のカウンター(17)を備え、前記乱数発生器から出力された前回の乱数データを保持するデータ保持器(8)を備え、前記乱数発生器から出力された今回の乱数データと前記データ保持器に保持された前回の乱数データとを比較して、両者が同一のときにカウントアップ信号を出力するとともに、両者が異なるときにカウントクリア信号を出力する比較器(9)を備え、前記比較器からカウントアップ信号を受けたときにカウントアップするとともに、前記比較器からカウントクリア信号を受けたときにカウントクリアする第2のカウンター(18)を備え、第2のカウンターの出力データをデコードして各信号長ごとに出力するデコーダー(19)を備え、このデコーダーの出力データを各信号長ごとにそれぞれカウントする複数個の第3のカウンター(20)を備え、第1のカウンターで計数された一定回数ごとに第3の各カウンターの出力データをそれぞれ保持する複数個のレジスタ(21)を備え、第1のカウンターで計数された一定回数ごとの信号と前記比較器の出力データとに基づいて前記各レジスタから検証データを出力するように制御する制御回路(22)を備えて構成される。

【0012】また、本発明のうち請求項7に係る発明は、上記レジスタ(21)の出力データを選択して出力する選択回路(23)を付設して構成される。

【0013】また、本発明のうち請求項8に係る発明は、上記1ビット乱数発生装置(1)を複数個並列に接続し、これら1ビット乱数発生装置から出力された検証データをビットごとに選択して出力する選択回路(26)を付設して構成される。

【0014】また、本発明のうち請求項9に係る発明は、上記1ビット乱数発生装置(24)を複数個並列に接続し、これら1ビット乱数発生装置から出力された検証信号をビットごとに選択して出力する選択回路(2

7)を付設して構成される。

【0015】また、本発明のうち請求項10に係る発明は、上記1ビット乱数発生装置(1、24)を有し、この1ビット乱数発生装置から出力された乱数データをシリアルデータからパラレルデータへ変換するシフトレジスタ(31)を備え、一定のパラレルデータのビット長を計数するカウンター(32)を備え、このカウンターで計数された周期ごとに前記シフトレジスタのパラレルデータを保持するレジスタ(33)を備え、予め設定された確率上限データおよび確率下限データと前記レジスタに保持されたパラレルデータとを比較して確率信号を出力する比較器(34)を備えて構成される。

【0016】さらに、本発明のうち請求項11に係る発明は、上記多数ビット乱数発生装置(25)を有し、予め設定された確率上限データおよび確率下限データと前記多数ビット乱数発生装置から出力された乱数データとを比較して確率信号を出力する比較器(35)を備えて構成される。

【0017】これらの構成において、データ保持器の代表例としてDタイプフリップフロップを挙げることができ、比較器の代表例としては排他的論理和素子(EXCLUSIVE-OR素子)を挙げることができる。そして、こうした構成を採用することにより、乱数データの出現一様性を自ら検証することが可能となり、使用者が統計処理を行う必要がなくなるように作用する。

【0018】なお、括弧内の符号は図面において対応する要素を表す便宜的なものであり、したがって、本発明は図面上の記載に限定拘束されるものではない。このことは「特許請求の範囲」の欄についても同様である。

【0019】

【発明の実施の形態】以下、本発明の実施形態を図面に基いて説明する。

【0020】図1は本発明に係る1ビット乱数発生装置の第1の実施形態を示す回路図である。

【0021】この1ビット乱数発生装置1は、図1に示すように、乱数発生器2、第1のカウンター3、第2のカウンター4、レジスタ5および出力回路6から構成された検証データ出力型であり、乱数発生器2に同期信号が入力されると、乱数発生器2から乱数データとして「1」または「0」が出力される。このとき、乱数発生器2の入力信号が第1のカウンター3にも入力され、第1のカウンター3は一定回数を計数して第2のカウンター4およびレジスタ5に出力する。一方、第2のカウンター4は、乱数発生器2から出力された乱数データの出現回数を計数して回数データを生成する。そして、レジスタ5は、第1のカウンター3で計数された周期ごとに第2のカウンター4の回数データを保持し、出力回路6は、レジスタ5に保持された回数データを検証データとしてシリアルまたはパラレルに出力する。

【0022】したがって、この1ビット乱数発生装置1

では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を自ら検証することが可能となる。

【0023】図2は本発明に係る1ビット乱数発生装置の第2の実施形態を示す回路図である。

【0024】この1ビット乱数発生装置24は、図2に示すように、乱数発生器2、第1のカウンター3、第2のカウンター4、レジスター5および比較器7から構成された検証信号出力型であり、乱数発生器2に同期信号が入力されると、乱数発生器2から乱数データとして「1」または「0」が出力される。このとき、乱数発生器2の入力信号が第1のカウンター3にも入力され、第1のカウンター3は一定回数を計数する。一方、第2のカウンター4は、乱数発生器2から出力された乱数データの出現回数を計数して回数データを生成する。そして、レジスター5は、第1のカウンター3で計数された周期ごとに第2のカウンター4の回数データを保持する。さらに、比較器7は、レジスター5に保持されたデータと予め設定された上限比較データおよび下限比較データとを比較し、レジスター5内のデータが上限比較データと下限比較データとの間にある場合には乱数データの出現一様性が高い旨の検証信号を出力し、それ以外の場合には乱数データの出現一様性が低い旨の検証信号を出力する。

【0025】したがって、この1ビット乱数発生装置24では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を自ら検証することが可能となる。

【0026】図3は本発明に係る1ビット乱数発生装置の第3の実施形態を示す回路図である。

【0027】この1ビット乱数発生装置1は、乱数発生器2の出力が一様であれば“0”または“1”が出る確率は $1/2$ であるため、各々の数字が $k$ 回連続して出現する確率は $(1/2)^k$ であり、例えば30回連続して同じ数字が出現する確率は $1/1073741824$ （すなわち、ほとんどゼロ）となるので、もし30回連続して同じ数字が出現したら、この乱数発生器2は正常ではないと判断できるという考え方に基づくものである。

【0028】すなわち、この1ビット乱数発生装置1は、図3に示すように、乱数発生器2、Dタイプフリップフロップなどのデータ保持器8、排他的論理和素子などの比較器9、カウンター10および出力回路6から構成された検証データ出力型であり、乱数発生器2に同期信号が入力されると、乱数発生器2から乱数データとして「1」または「0」が出力される。このとき、乱数発生器2の入力信号および出力信号がデータ保持器8にも入力され、データ保持器8は、乱数発生器2から出力された前回の乱数データを保持して比較器9に出力する。また、比較器9には乱数発生器2の出力信号も入力さ

れ、比較器9は、乱数発生器2から出力された今回の乱数データとデータ保持器8に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号をカウンター10に出力するとともに、両者が異なるときにはカウントクリア信号をカウンター10に出力する。そして、カウンター10には乱数発生器2の入力信号も入力され、カウンター10はそのデータを出力回路6に出力し、出力回路6はそのデータを同一信号長の検証データとしてシリアルまたはパラレルに逐次出力する。

【0029】したがって、この1ビット乱数発生装置1では、出力された同一信号長の検証データによって、乱数の一様性を検証するための統計処理が容易になる。

【0030】図4は本発明に係る1ビット乱数発生装置の第4の実施形態を示す回路図である。

【0031】この1ビット乱数発生装置1は、図4に示すように、乱数発生器2、Dタイプフリップフロップなどのデータ保持器8、排他的論理和素子などの第1の比較器11、カウンター10、レジスター12、排他的論理和素子などの第2の比較器13、制御回路14および出力回路15から構成された検証データ出力型であり、乱数発生器2に同期信号が入力されると、乱数発生器2から乱数データとして「1」または「0」が出力される。このとき、乱数発生器2の入力信号および出力信号がデータ保持器8にも入力され、データ保持器8は、乱数発生器2から出力された前回の乱数データを保持して第1の比較器11に出力する。また、第1の比較器11には乱数発生器2の出力信号も入力され、第1の比較器11は、乱数発生器2から出力された今回の乱数データとデータ保持器8に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号をカウンター10に出力するとともに、両者が異なるときにはカウントクリア信号をカウンター10に出力する。そして、カウンター10には乱数発生器2の入力信号も入力され、カウンター10はそのデータを第2の比較器13に出力し、第2の比較器13は、レジスター12のデータとカウンター10の出力データとを比較し、前者より後者の方が大きいときにはデータ上書き信号を制御回路14に出力するとともに、それ以外のときにはデータ保持信号を制御回路14に出力する。制御回路14は、データ上書き信号を受けたときにはカウンター10の出力データをレジスター12に書き込むとともに、データ保持信号を受けたときにはレジスター12のデータを保持するように制御し、出力回路15は、レジスター12に保持されたデータを最長の同一信号長の検証データとしてシリアルまたはパラレルに逐次出力する。

【0032】したがって、この1ビット乱数発生装置1では、出力された最長の同一信号長の検証データによって、乱数の一様性を検証するための統計処理が容易になる。

【0033】図5は本発明に係る1ビット乱数発生装置の第5の実施形態を示す回路図である。

【0034】この1ビット乱数発生装置24は、図5に示すように、乱数発生器2、Dタイプフリップフロップなどのデータ保持器8、排他的論理和素子などの第1の比較器11、カウンタ10、レジスタ12、排他的論理和素子などの第2の比較器13、制御回路14および排他的論理和素子などの第3の比較器16から構成された検証信号出力型であり、乱数発生器2に同期信号が入力されると、乱数発生器2から乱数データとして「1」または「0」が出力される。このとき、乱数発生器2の入力信号および出力信号がデータ保持器8にも入力され、データ保持器8は、乱数発生器2から出力された前回の乱数データを保持して第1の比較器11に出力する。また、第1の比較器11には乱数発生器2の出力信号も入力され、第1の比較器11は、乱数発生器2から出力された今回の乱数データとデータ保持器8に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号をカウンタ10に出力するとともに、両者が異なるときにはカウントクリア信号をカウンタ10に出力する。そして、カウンタ10には乱数発生器2の入力信号も入力され、カウンタ10はそのデータを第2の比較器13に出力し、第2の比較器13は、レジスタ12のデータとカウンタ10の出力データとを比較し、前者より後者の方が大きいときにはデータ上書き信号を制御回路14に出力するとともに、それ以外のときにはデータ保持信号を制御回路14に出力する。制御回路14は、データ上書き信号を受けたときにはカウンタ10の出力データをレジスタ12に書き込むとともに、データ保持信号を受けたときにはレジスタ12のデータを保持するように制御し、第3の比較器16は、レジスタ12に保持されたデータと予め設定された比較データとを比較して最長の同一信号長の検証信号を逐次出力する。

【0035】したがって、この1ビット乱数発生装置24では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を自ら検証することが可能となる。

【0036】図6は本発明に係る1ビット乱数発生装置の第6の実施形態を示す回路図である。

【0037】この1ビット乱数発生装置1は、図6に示すように、乱数発生器2、Dタイプフリップフロップなどのデータ保持器8、排他的論理和素子などの比較器9、第1のカウンタ17、第2のカウンタ18、デコーダ19、複数個(n個)の第3のカウンタ20、複数個(n個)のレジスタ21および制御回路22から構成された検証データ出力型であり、乱数発生器2に同期信号が入力されると、乱数発生器2から乱数データとして「1」または「0」が出力される。このとき、第1のカウンタ17が計数する一定回数での各同一信号長(1~n)の出現率をカウントし、第1のカウンタ17が計数する一定回数ごとにレジスタ21に書き込み、各同一信号長の分布を外部からの選択データで選択できる選択回路23にて逐次出力する。

一信号長(1~n)の出現率をカウントし、第1のカウンタ17が計数する一定回数ごとにレジスタ21に書き込み、各同一信号長の分布を逐次出力する。

【0038】すなわち、乱数発生器2の入力信号および出力信号がデータ保持器8にも入力され、データ保持器8は、乱数発生器2から出力された前回の乱数データを保持して比較器9に出力する。また、比較器9には乱数発生器2の出力信号も入力され、比較器9は、乱数発生器2から出力された今回の乱数データとデータ保持器8に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号を制御回路22に出力するとともに、両者が異なるときにはカウントクリア信号を制御回路22に出力する。一方、乱数発生器2の入力信号は第1のカウンタ17および制御回路22にも入力され、第1のカウンタ17は一定回数を計数して制御回路22に出力する。さらに、乱数発生器2の入力信号は第2のカウンタ18にも入力され、第2のカウンタ18は、比較器9からカウントアップ信号を受けたときにはカウントアップしてデコーダ19に出力するとともに、比較器9からカウントクリア信号を受けたときにはカウントクリアしてデコーダ19に出力する。これを受けてデコーダ19は、第2のカウンタ18の出力データをデコードして各信号長ごとに第3の各カウンタ20へ出力し、各カウンタ20はこの出力データをカウントして各レジスタ21に出力する。そして、各レジスタ21は、制御回路22による制御下で、比較器9の出力データと第1のカウンタ17で計数された一定回数ごとの信号とに基づいて同一信号長の検証データをシリアルまたはパラレルに逐次出力する。

【0039】したがって、この1ビット乱数発生装置1では、出力された各カウント数(検証データ)によって、乱数の一様性を検証するための統計処理が容易になる。

【0040】図7は本発明に係る1ビット乱数発生装置の第7の実施形態を示す回路図である。

【0041】この1ビット乱数発生装置1は、図7に示すように、乱数発生器2、Dタイプフリップフロップなどのデータ保持器8、排他的論理和素子などの比較器9、第1のカウンタ17、第2のカウンタ18、デコーダ19、複数個(n個)の第3のカウンタ20、複数個(n個)のレジスタ21、制御回路22および選択回路23から構成された検証データ出力型であり、乱数発生器2に同期信号が入力されると、乱数発生器2から乱数データとして「1」または「0」が出力される。このとき、第1のカウンタ17が計数する一定回数での各同一信号長(1~n)の出現率をカウントし、第1のカウンタ17が計数する一定回数ごとにレジスタ21に書き込み、各同一信号長の分布を外部からの選択データで選択できる選択回路23にて逐次出力する。



【0042】すなわち、乱数発生器2の入力信号および出力信号がデータ保持器8にも入力され、データ保持器8は、乱数発生器2から出力された前回の乱数データを保持して比較器9に出力する。また、比較器9には乱数発生器2の出力信号も入力され、比較器9は、乱数発生器2から出力された今回の乱数データとデータ保持器8に保持された前回の乱数データとを比較し、両者が同一のときにはカウントアップ信号を制御回路22に出力するとともに、両者が異なるときにはカウントクリア信号を制御回路22に出力する。一方、乱数発生器2の入力信号は第1のカウンター17および制御回路22にも入力され、第1のカウンター17は一定回数を計数して制御回路22に出力する。さらに、乱数発生器2の入力信号は第2のカウンター18にも入力され、第2のカウンター18は、比較器9からカウントアップ信号を受けたときにはカウントアップしてデコーダー19に出力するとともに、比較器9からカウントクリア信号を受けたときにはカウントクリアしてデコーダー19に出力する。これを受けてデコーダー19は、第2のカウンター18の出力データをデコードして各信号長ごとに第3の各カウンター20へ出力し、各カウンター20はこの出力データをカウントして各レジスター21に出力する。そして、各レジスター21は、制御回路22による制御下で、比較器9の出力データと第1のカウンター17で計数された一定回数ごとの信号とに基づいて同一信号長の検証データを選択回路23にシリアルまたはパラレルに逐次出力する。さらに、選択回路23に外部から選択データが入力されると、選択回路23はレジスター21の出力データをその選択データに基づいて適宜選択して出力する。

【0043】したがって、この1ビット乱数発生装置1では、出力された同一信号長の分布データによって、乱数の一様性を検証するための統計処理が容易になる。

【0044】図8は本発明に係る多数ビット乱数発生装置の第1の実施形態を示す回路図である。

【0045】この多数ビット乱数発生装置25は、図8に示すように、上述した検証データ出力型の1ビット乱数発生装置1を複数個(n個)並列に接続し、これに選択回路26を付設したものであり、選択回路26に外部から選択データが入力されると、選択回路26は、1ビット乱数発生装置1から出力された検証データをその選択データに基づいてビットごとに選択して出力する。

【0046】したがって、この多数ビット乱数発生装置25では、出力された一様性検証データによって、乱数の一様性を検証するための統計処理が容易になる。

【0047】図9は本発明に係る多数ビット乱数発生装置の第2の実施形態を示す回路図である。

【0048】この多数ビット乱数発生装置25は、図9に示すように、上述した検証信号出力型の1ビット乱数発生装置24を複数個(n個)並列に接続し、これに選

択回路27を付設したものであり、選択回路27に外部から選択データが入力されると、選択回路27は、1ビット乱数発生装置24から出力された検証信号をその選択データに基づいてビットごとに選択して出力する。

【0049】したがって、この多数ビット乱数発生装置25では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を自ら検証することが可能となる。

【0050】図10は本発明に係る確率発生装置の第1の実施形態を示す回路図である。

【0051】この確率発生装置30は、図10に示すように、上述した検証データ出力型の1ビット乱数発生装置1、シフトレジスター31、カウンター32、レジスター33および比較器34から構成されており、1ビット乱数発生装置1から出力された乱数データはシフトレジスター31に入力され、シフトレジスター31はこの乱数データをシリアルデータからパラレルデータへ変換してレジスター33に出力する。一方、1ビット乱数発生装置1の入力信号はカウンター32にも入力され、カウンター32は一定のパラレルデータのビット長を計数してレジスター33に出力する。すると、レジスター33は、カウンター32で計数された周期ごとにシフトレジスター31のパラレルデータを保持する。そして、比較器34は、レジスター33に保持されたデータと予め設定された確率上限データおよび確率下限データとを比較し、レジスター33内のデータが確率上限データと確率下限データとの間にある場合には“当たり”、それ以外の場合には“外れ”の確率信号を出力する。

【0052】したがって、この確率発生装置30では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を検証することが容易であることから、確率の信頼性を評価することも容易になる。

【0053】図11は本発明に係る確率発生装置の第2の実施形態を示す回路図である。

【0054】この確率発生装置30は、図11に示すように、上述した検証信号出力型の1ビット乱数発生装置24、シフトレジスター31、カウンター32、レジスター33および比較器34から構成されており、1ビット乱数発生装置24から出力された乱数データはシフトレジスター31に入力され、シフトレジスター31はこの乱数データをシリアルデータからパラレルデータへ変換してレジスター33に出力する。一方、1ビット乱数発生装置24の入力信号はカウンター32にも入力され、カウンター32は一定のパラレルデータのビット長を計数してレジスター33に出力する。すると、レジスター33は、カウンター32で計数された周期ごとにシフトレジスター31のパラレルデータを保持する。そして、比較器34は、レジスター33に保持されたデータと予め設定された確率上限データおよび確率下限データとを比較し、レジスター33内のデータが確率上限デー



タと確率下限データとの間にある場合には“当たり”、それ以外の場合には“外れ”の確率信号を出力する。

【0055】したがって、この確率発生装置30では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を検証することが容易であることから、確率の信頼性を評価することも容易になる。

【0056】図12は本発明に係る確率発生装置の第3の実施形態を示す回路図、図13は本発明に係る確率発生装置の第4の実施形態を示す回路図である。

【0057】これらの確率発生装置30は、図12および図13に示すように、上述した多数ビット乱数発生装置25および比較器35から構成されており、多数ビット乱数発生装置25から出力された乱数データ（パレルデータ）は比較器35に入力され、比較器35は、この乱数データと予め設定された確率上限データおよび確率下限データとを比較し、乱数データが確率上限データと確率下限データとの間にある場合には“当たり”、それ以外の場合には“外れ”の確率信号を出力する。

【0058】したがって、この確率発生装置30では、使用者が面倒で煩雑な統計処理を行わなくても乱数データの出現一様性を検証することが容易であることから、確率の信頼性を評価することも容易になる。

【0059】

【発明の効果】以上説明したように、本発明のうち請求項1〜7に係る発明によれば、乱数データの出現一様性を自ら検証することができ、使用者が統計処理を行う必要がなくなることから、乱数データの出現一様性を手軽に検証して信頼性を高めることが可能な1ビット乱数発生装置を提供することができる。

【0060】また、本発明のうち請求項8、9に係る発明によれば、乱数データの出現一様性を自ら検証することができ、使用者が統計処理を行う必要がなくなることから、乱数データの出現一様性を手軽に検証して信頼性を高めることが可能な多数ビット乱数発生装置を提供することができる。

【0061】さらに、本発明のうち請求項10、11に係る発明によれば、乱数データの出現一様性を自ら検証することができ、使用者が統計処理を行う必要がなくなることから、乱数データの出現一様性を手軽に検証して信頼性を高めることが可能な確率発生装置を提供することができる。

【図面の簡単な説明】

【図1】本発明に係る1ビット乱数発生装置の第1の実施形態を示す回路図である。

【図2】本発明に係る1ビット乱数発生装置の第2の実施形態を示す回路図である。

【図3】本発明に係る1ビット乱数発生装置の第3の実施形態を示す回路図である。

【図4】本発明に係る1ビット乱数発生装置の第4の実施形態を示す回路図である。

【図5】本発明に係る1ビット乱数発生装置の第5の実施形態を示す回路図である。

【図6】本発明に係る1ビット乱数発生装置の第6の実施形態を示す回路図である。

【図7】本発明に係る1ビット乱数発生装置の第7の実施形態を示す回路図である。

【図8】本発明に係る多数ビット乱数発生装置の第1の実施形態を示す回路図である。

【図9】本発明に係る多数ビット乱数発生装置の第2の実施形態を示す回路図である。

【図10】本発明に係る確率発生装置の第1の実施形態を示す回路図である。

【図11】本発明に係る確率発生装置の第2の実施形態を示す回路図である。

【図12】本発明に係る確率発生装置の第3の実施形態を示す回路図である。

【図13】本発明に係る確率発生装置の第4の実施形態を示す回路図である。

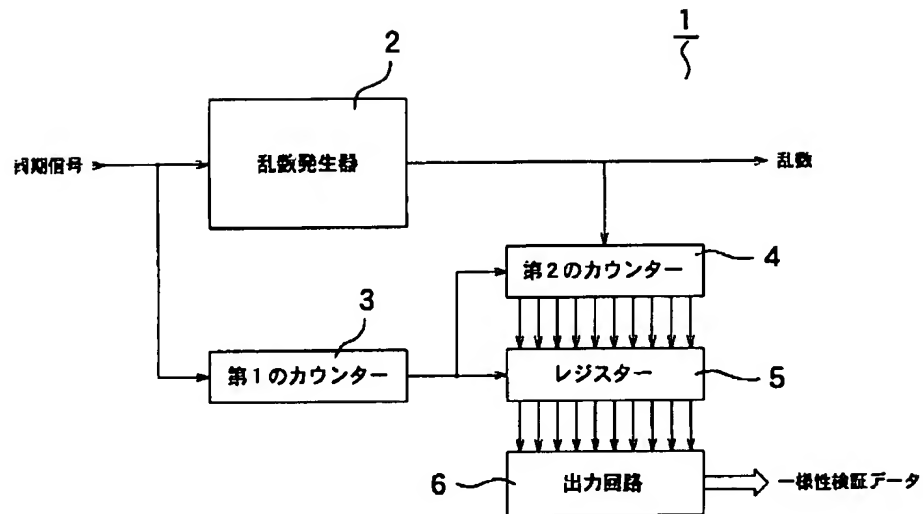
【符号の説明】

- 1……1ビット乱数発生装置
- 2……乱数発生器
- 3……第1のカウンター
- 4……第2のカウンター
- 5……レジスター
- 6……出力回路
- 7……比較器
- 8……データ保持器
- 9……比較器
- 10……カウンタ
- 11……第1の比較器
- 12……レジスター
- 13……第2の比較器
- 14……制御回路
- 15……出力回路
- 16……第3の比較器
- 17……第1のカウンター
- 18……第2のカウンター
- 19……デコーダ
- 20……第3のカウンター
- 21……レジスター
- 22……制御回路
- 23……選択回路
- 24……1ビット乱数発生装置
- 25……多数ビット乱数発生装置
- 26……選択回路
- 27……選択回路
- 30……確率発生装置
- 31……シフトレジスター
- 32……カウンタ
- 33……レジスター

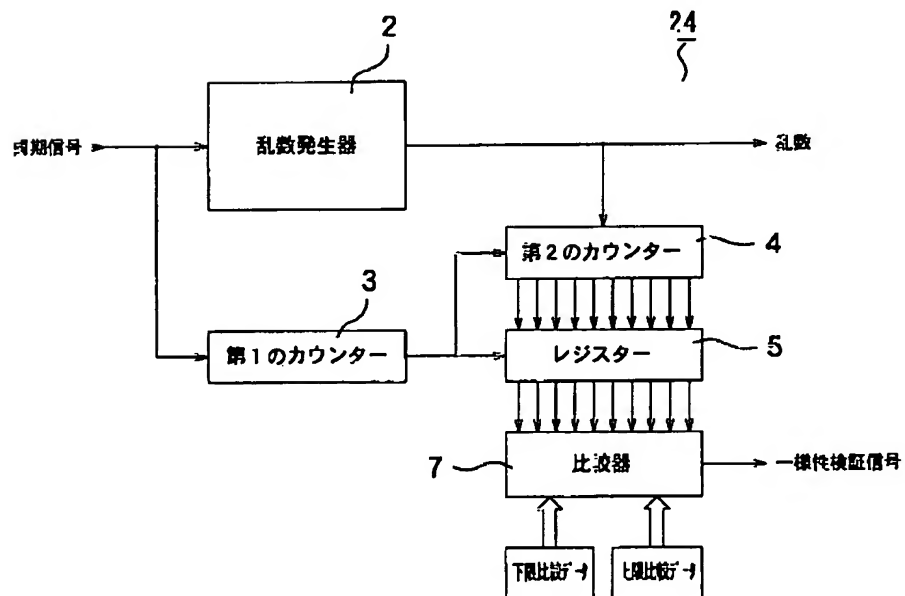
34……比較器

35……比較器

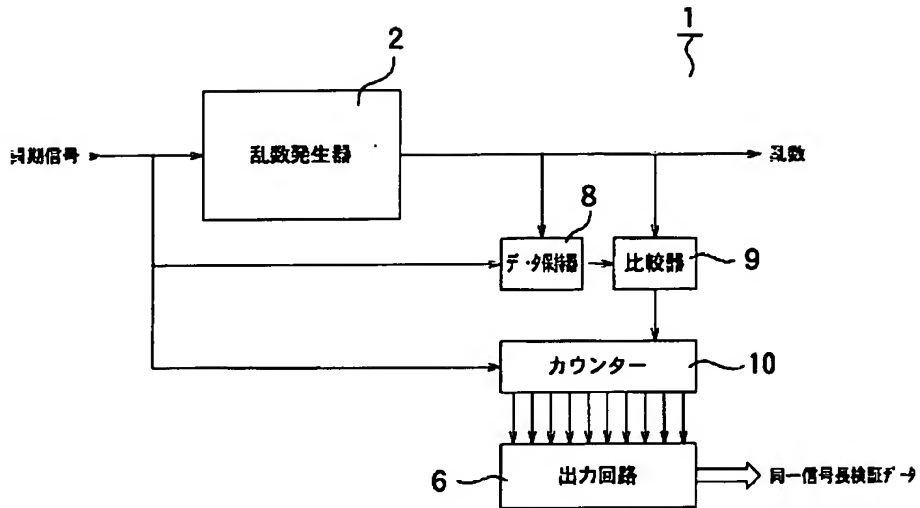
【図1】



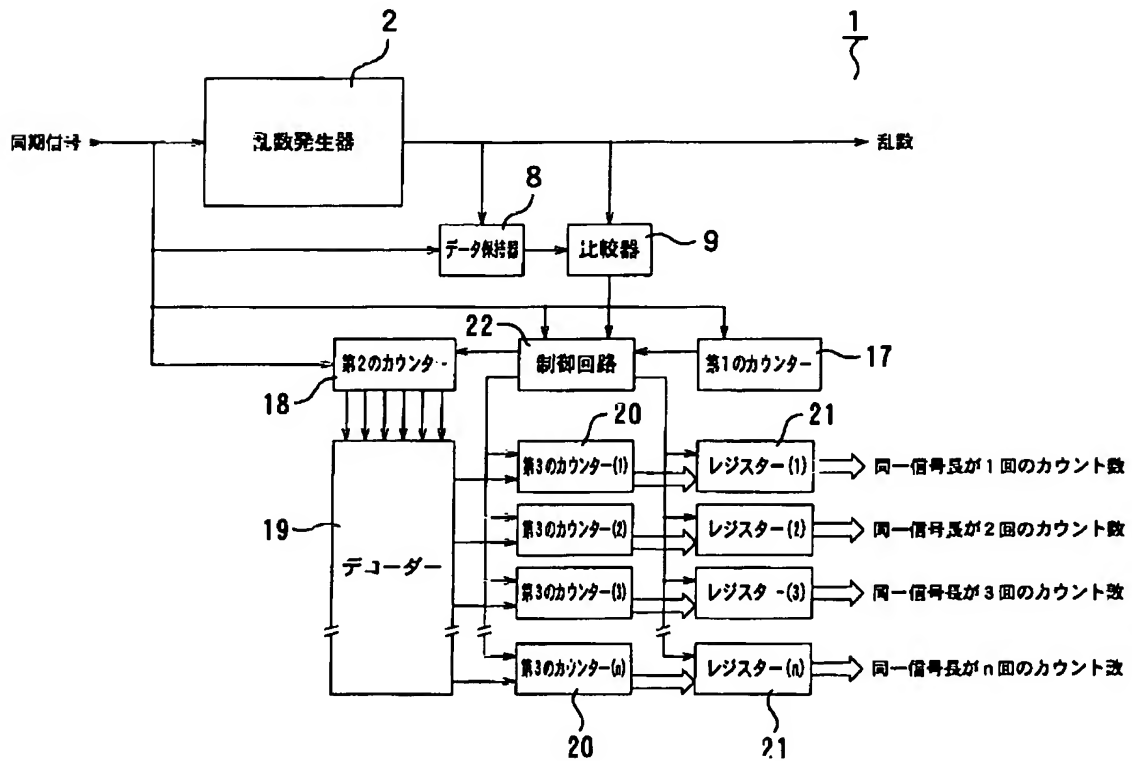
【図2】



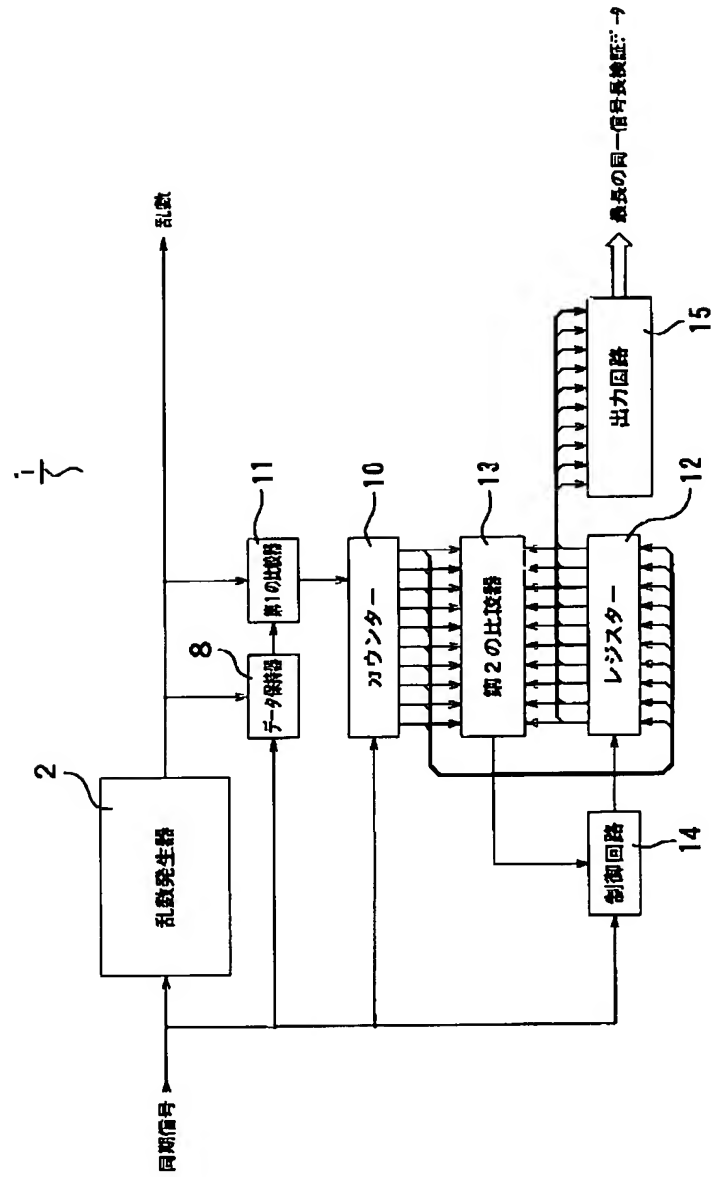
【図3】



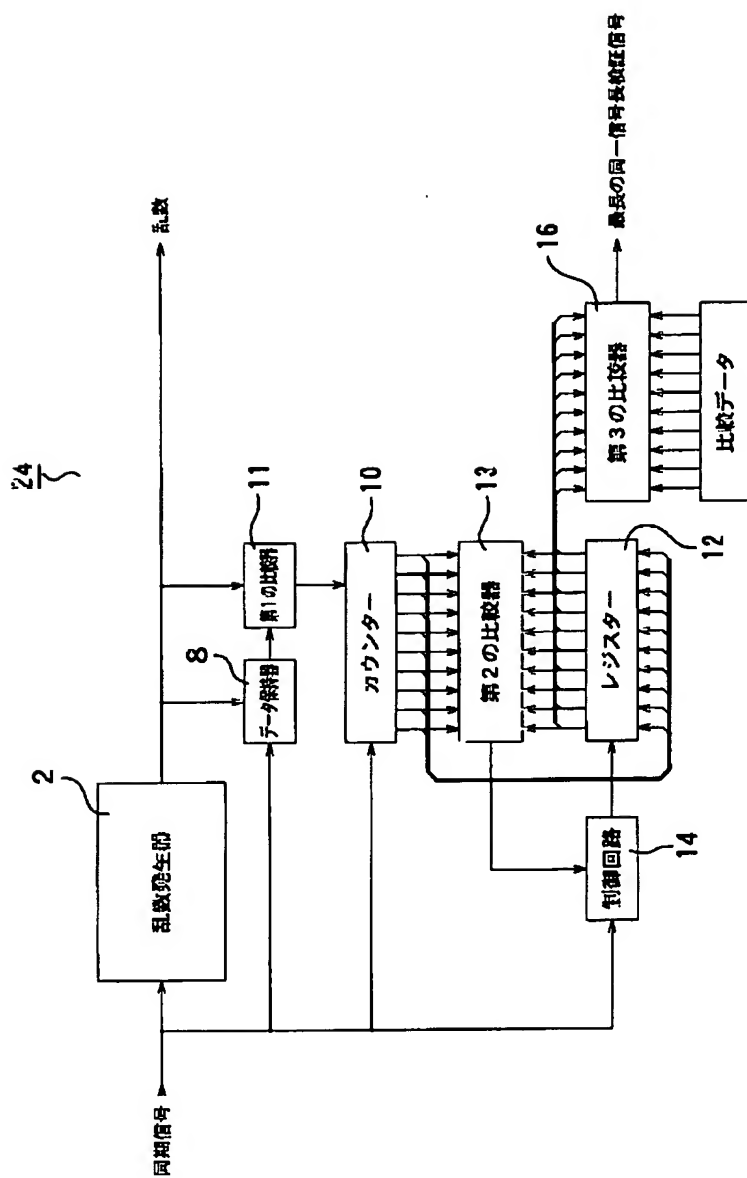
【図6】



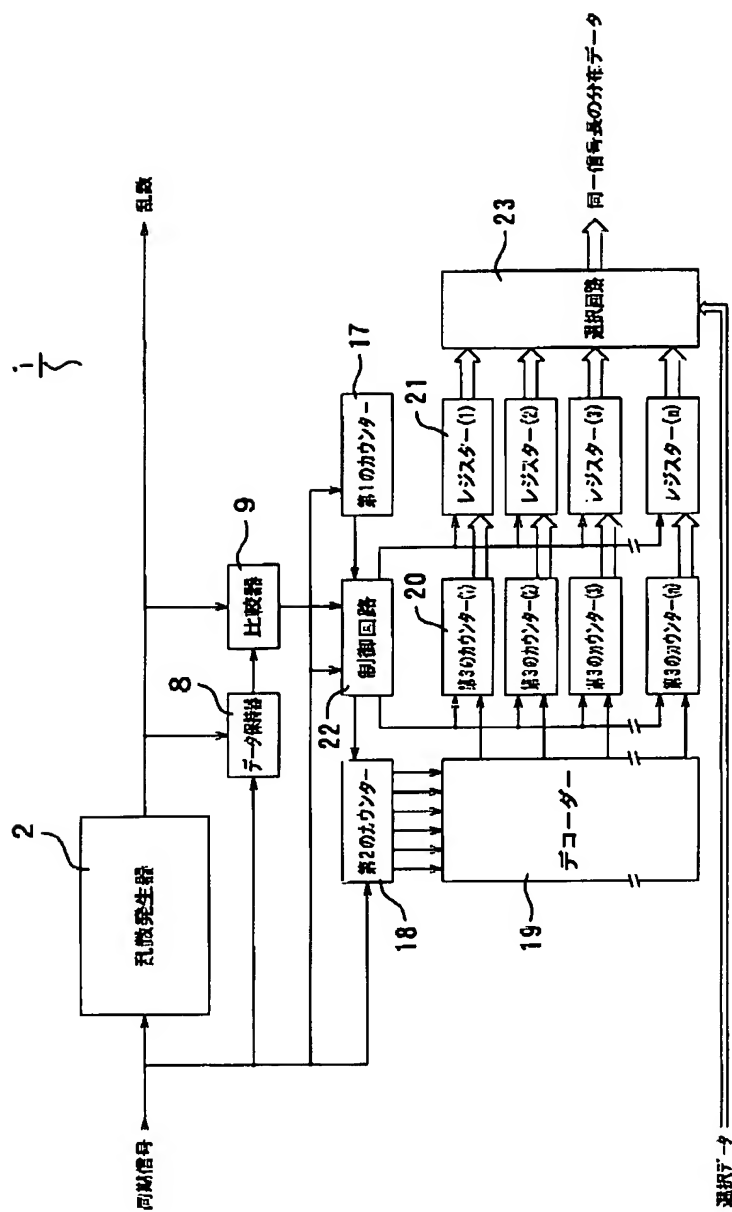
【図4】



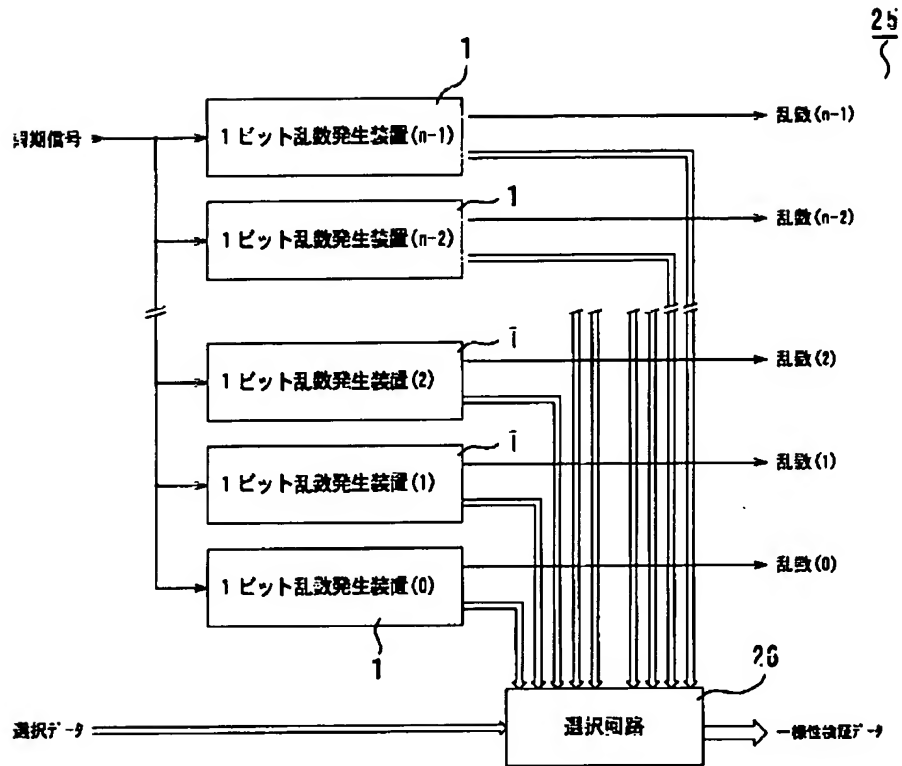
【図5】



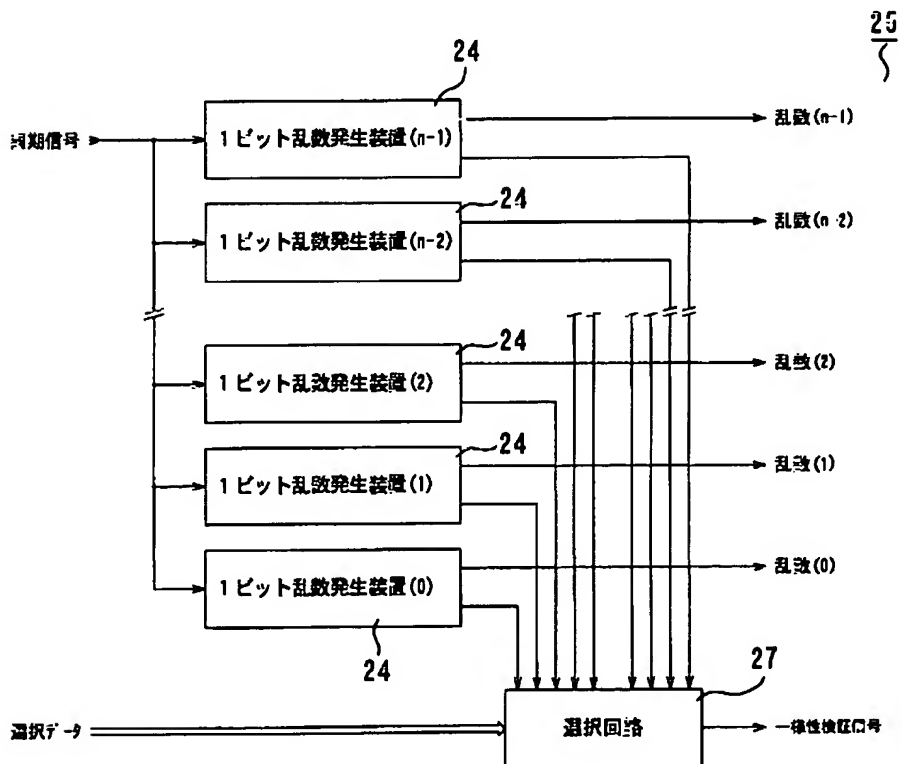
【図7】



【図8】

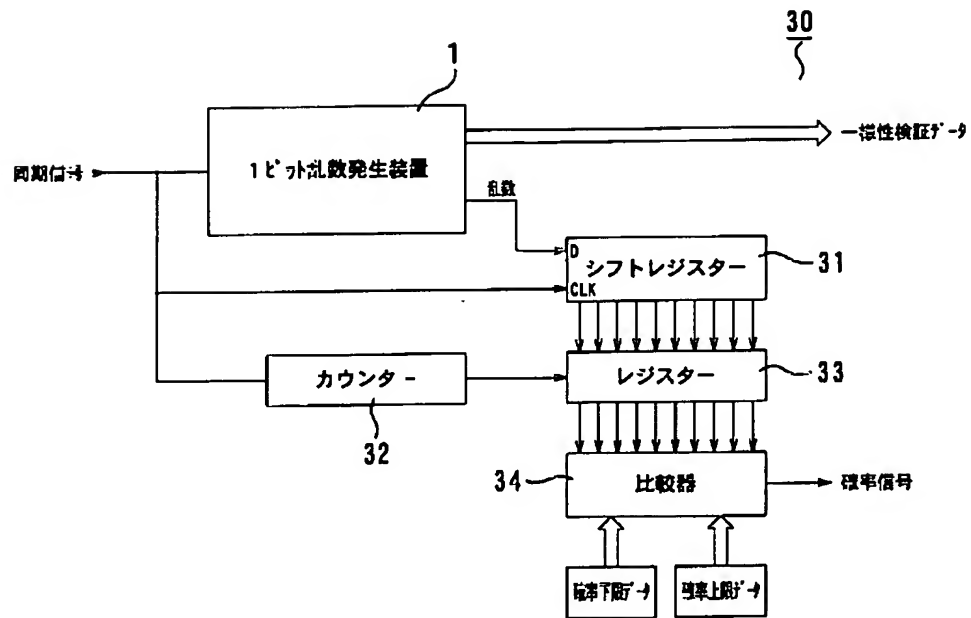


【図9】

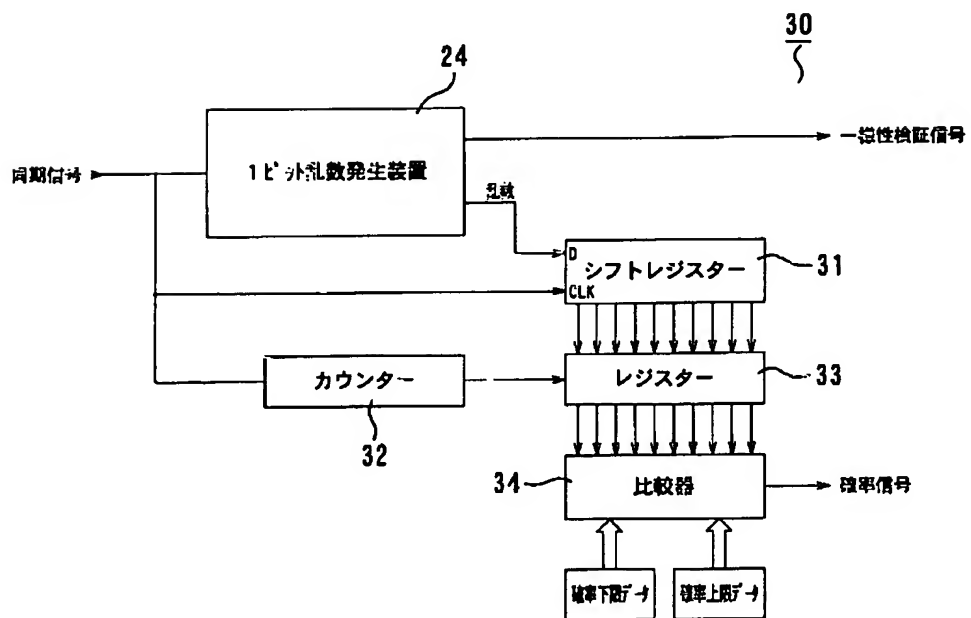




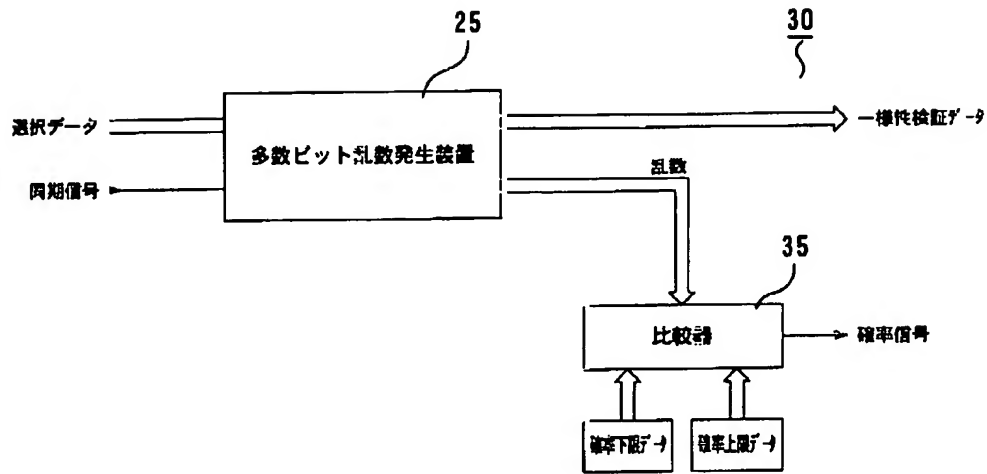
【図10】



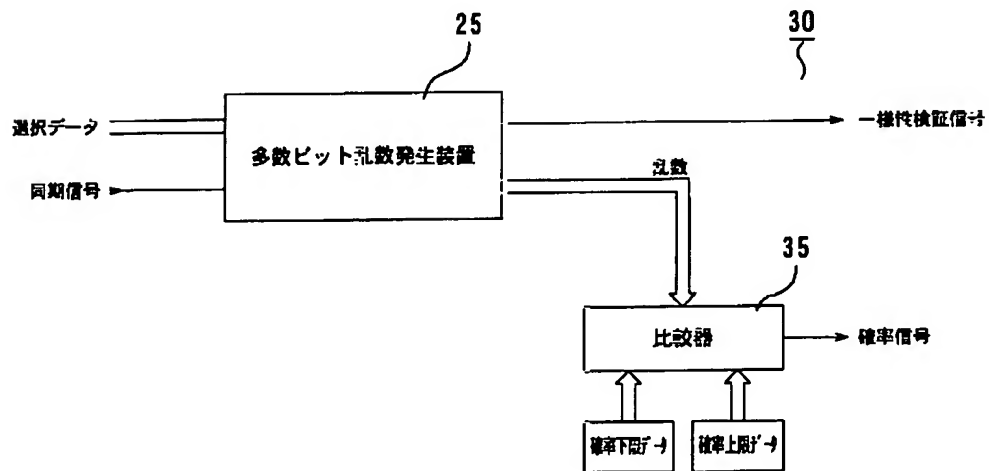
【図11】



【図12】



【図13】



フロントページの続き

(72)発明者 清水 隆邦  
東京都港区新橋5丁目36番11号 いわき電  
子株式会社内

(72)発明者 蛭淵 美佐子  
東京都港区新橋5丁目36番11号 いわき電  
子株式会社内  
Fターム(参考) 5J104 FA00 GA00